BMWK Projekt:

“ Robuste Laufzeitüberwachung mittels nachvollziehbarer Zustandsanalyse für den hoch-kritischen eVOTL-Betrib (20Q1963C)”

Schlussbericht

Teil I: Kurzbericht mit einer kurzen Darstellung der bisherigen Projektergebnisse

Aufgabenstellung

Das übergeordnete Ziel des Verbundvorhabens „*voloSTREAM*“ ist die automatische Überwachung sicherheitsrelevanter Aspekte eines hochautomatisierten elektrischen Luftfahrzeugs. Ziel des CISPA-Anteils ist die Erforschung von theoretischen Grundlagen zur Laufzeitüberwachung. Die Grundlagen wurden in mehreren Prototypen realisiert und in unbemannten Luftfahrzeugen von dem DLR und Volocopter integriert. Das Vorhaben gliederte sich somit in folgende Teilziele:

- Erforschung der Grundlagen der fehlertoleranten, nachvollziehbaren Laufzeitüberwachung
- Weiterentwicklung der Spezifikationssprache
- Entwicklung von lauffähigen Monitorprototypen

Voraussetzungen

Prof. Bernd Finkbeiner leitet seit 2002 die Reactive Systems Group der Universität. Die Forschungsgruppe beschäftigt sich mit drei Formen der Analyse von verteilten, robusten, reaktiven Systemen: Die statische Verifikation mittels Model-Checking, die statische Konstruktion mittels Programmsynthese und die dynamische Verifikation mittels Laufzeitüberwachung. Zu den wichtigsten Arbeitsbereichen der Forschungsgruppe zählt die formale Spezifikationssprache “Lola”. Lola erlaubt mathematisch-präzise Modelle des Systemverhaltens. Prototypisch ist es bereits gelungen, aus Spezifikationen automatisch Monitorkomponenten zu generieren, die ein Fehlverhalten des Systems früh erkennen. In Kooperation mit dem Deutschen Zentrum für Luft- und Raumfahrt wurde Lola erfolgreich zur Überwachung autonomer Drohnen eingesetzt. Die Kooperation führte zu einer Abschlussarbeit und mehreren Publikationen. Die Gruppe ist regelmäßig an Sonderforschungsbereichen beteiligt, darunter AVACS (Automatic Verification and Analysis of Complex Systems, SFB/TR 14, 2004-2015), privacySFB (Methods and Tools for Understanding and Controlling Privacy, SFB 1223, 2016-2019) und Foundations of Perspicuous Software Systems (DFG CRC 248, 2019-2026). Im Jahr 2016 wurde die Forschung von Prof. Finkbeiner mit einem ERC Consolidator Grant ausgezeichnet. In dem ERC-Projekt OSARES (Output-Sensitive Algorithms for Reactive Synthesis) werden neuartige Algorithmen für die automatische Konstruktion korrekter Software aus formalen Spezifikationen entwickelt. Im Jahr 2022 wurde seine Forschung mit dem ERC Advanced Grant

ausgezeichnet. Ziel des Projektes HYPER ist es, eine Spezifikationssprache zu entwickeln, mit der auch komplexe gesellschaftliche Konzepte wie Gerechtigkeit, Privatsphäre oder Erklärbarkeit mathematisch formalisiert werden können.

Planung und Ablauf des Vorhabens

Das Projekt war in 6 Hauptarbeitspakete (HAP) unterteilt:

- HAP 0 – Management
- HAP 1 – Systemanforderung und Design
- HAP 2 – RV Technik
- HAP 3 – Volocopter RV Integration
- HAP 4 – Systemvalidierung
- HAP 5 – Zertifizierungsaspekte

Das CISPA leitete das HAP 2 und beteiligte sich an HAP 3 und HAP 5. Gegen Ende des Vorhabens wurde ein Antrag auf eine kostenneutrale Laufzeitverlängerung um 6 Monate gestellt, welcher akzeptiert wurde. In diesem Antrag bekamen die Use-cases der Laufzeitüberwachung einen neuen Zeitplan, um die Flugversuche zu realisieren. An der übergeordneten Aufgabenstellung hat sich nichts verändert.

Im Nachfolgenden geben wir eine kurze Übersicht über die Ergebnisse an den vom CISPA beteiligten HAPs.

HAP 2 – RV Technik

HAP 2 beschäftigte sich mit den Grundlagen für eine formale, ausdrucksstarke Spezifikationssprache brachte diese in den domänenspezifischen Kontext. Außerdem wird die Robustheit, d.h. Fehlertoleranz des Monitors und der Zusammenhang zwischen der formalen Spezifikation und dem resultierenden Monitor untersucht. In diesem Arbeitspaket wurden 4 Prototypen entwickelt: MS 2.1 Prototype für Logfileanalyse, MS 2.2 Prototype für Laufzeitüberwachung, MS 2.3 Fehlertoleranter Prototype und MS 2.4 Nachvollziehbarer Prototype entwickelt. MS 2.1 und MS 2.2 sind auf crates.io veröffentlicht. Außerdem wurde in diesem Arbeitspaket eine Übersicht über den Stand der Forschung erstellt und es entstanden mehrere wissenschaftliche Publikationen [1] [2] [3] [4] [5].

HAP 3 – Volocopter RV Integration

Dieser HAP befasste sich mit der Integration eines Monitors in ein bestehendes System. Dazu werden beobachtete Eigenschaften formal ausgedrückt, nach Bedeutung geordnet und anschließend in unbemannte Fluggeräte integriert. Das CISPA als Entwickler der Sprache war unterstützenden an diesem HAP beteiligt. In dem Arbeitspaket fanden zwei Flugversuche statt: ein Flugversuch beim DLR und ein Flugversuch bei Volocopter. Die Ergebnisse des Flugversuchens bei Volocopter wurden unter anderem bei der “International Conference on Computer-Aided Verification” veröffentlicht [2]. Für das Management der Spezifikationen entstanden ebenfalls wissenschaftliche Publikationen [6] [7].

HAP 5 – Zertifizierungsaspekte

Ziel diese HAP war die Zertifizierung der Überwachungseinheit. Hier lag der Fokus des CISPAs auf der Nachvollziehbarkeit zwischen der Spezifikationssprache und des resultierenden Monitors. Die Ergebnisse dieses Arbeitspaketes sind beim dem “AIAA Science and Technology Forum and Exposition (AIAA SciTech Forum)” [8] veröffentlicht.

Stand der Wissenschaft und Technik

Um formale Laufzeitüberwachung zu nutzen, muss eine formale Spezifikationssprache verwendet werden. Diese muss ausdrucksstark genug sein, um komplexe Eigenschaften auszudrücken und gleichzeitig formal Garantieren einzuhalten. Eine Möglichkeit hierzu sind strombasierte Spezifikationssprachen wie Lola. Lola wurde ursprünglich zur Überwachung von digitalen Schaltkreisen entwickelt und besitzt hierfür die Annahme, dass alle einkommenden Daten gleichzeitig empfangen werden. Diese Annahme hält im Allgemeinen allerdings nicht in einer physischen Umgebung und schränkt somit die Ausdrucksmächtigkeit der Sprache ein. Neben Lola existieren noch andere strombasierte Spezifikationssprachen und eine detaillierte Übersicht über den Stand der Wissenschaft wurde vom CISPA im HAP 2 erstellt.

Zusammenarbeit

Innerhalb des Forschungsvorhabens arbeiteten die Verbundpartner Volocopter, CISPA und DLR eng zusammen und bündeln ihre Kompetenzen. Dies ermöglichte es, die Verbundvorhabenziele sowohl im Zeit- und Kostenrahmen, als auch qualitativ auf höchstem Niveau zu bearbeiten.

Für eine wissenschaftliche Publikation wurde außerdem mit der Iowa State University kollaboriert, die ebenfalls an der formalen Laufzeitüberwachung von unbemannten Luftfahrzeugen arbeiten.

BMWK Projekt:

“ Robuste Laufzeitüberwachung mittels nachvollziehbarer Zustandsanalyse für den hoch-kritischen eVOTL-Betrib (20Q1963C)”

Schlussbericht

Eingehende Darstellung

Verwendung der Zustellung

Hier geben wir einen detaillierteren Überblick über die Ergebnisse unserer Arbeit. Dabei werden nur die Arbeitspakete beschrieben an welchen das CISPA beteiligt war.

RV Technik (HAP 2)

Stand der Forschung (AP 2.1)

Dieses Arbeitspaket wird vom CISPA geleitet. Als Ergebnis dieses Arbeitspaketes entstand eine Übersicht über den Stand der Forschung, welche im Zwischenbericht Januar 2021 – Dezember 2021 dem Projektträger präsentiert wurde. Die entspricht dem ersten und einzigen Meilenstein dieses Arbeitspaketes.

Weiterentwicklung der Spezifikationssprache (AP 2.4)

Dieses Arbeitspaket wird vom CISPA geleitet und benutzt die Ergebnisse von AP 1.1 Spezifikationserhebung und AP 3.2 Formalisierung der Spezifikationseigenschaften. Wir analysierten die aufgestellten Eigenschaften, entwickelten neue Sprachkonstrukte für die Spezifikationssprache RTLola, die Spezifikationssprache welche in dem Projekt benutzt und erweitert wurde. Außerdem entstanden in diesem Arbeitspaket die Prototypen für die Logfileanalyse und die Laufzeitanalyse an (MS 2.1 und MS 2.2).

Neben größeren Erweiterungen der Sprache wurde im Projekt eine Menge an Sprachkonstrukten erarbeitet, die die Spezifikation leserlicher machen. Die größten Erweiterungen in diesem Arbeitspaket sind dynamische und parametrisierte Ströme, welche auf RTLola angepasst wurden. Außerdem wurde das Konzept der Instanzenaggregation eingeführt. Alle Erweiterungen haben Auswirkungen auf das Framework der Spezifikationssprache, wie das Typsystem, die Evaluierung und die Abhängigkeitsanalyse. Über die Erweiterungen entstand die Publikation [3] welche auf einer internationalen Konferenz veröffentlich werden soll. Außerdem entstanden durch den Abschluss von Arbeitspaket 1.1 und 3.2 eine große Menge an Spezifikationen und mit deren Komplexität das Problem des Spezifikationswartbarkeit. Zum Beispiel konnten wiederholende Muster in den Spezifikationen identifiziert werden, diese jedoch nicht in der Spezifikationssprache als solche ausgedrückt werden.

Dazu ist es häufig nötig verschiedene bereits formulierte Sicherheitseigenschaften in anderer Weise in einer neuen Spezifikation zu komponieren. Um diese Probleme zu lösen, wurde ein Konzept zur Modularisierung von Spezifikationen erarbeitet. Die Herausforderung bestand hierbei in dem strombasierten Berechnungsmodell der Spezifikationssprache RTLola, welches sich grundlegen von dem einer regulären Programmiersprache unterscheidet.

Die Meilensteile M2.1 Prototyp für die Logfileanalyse und M2.2 Prototyp sind öffentlich auf crates.io, werden stetig weiterentwickelt und kontinuierlich veröffentlicht. Um die Integration in die Volocopter Infrastruktur zu vereinfachen, modularer und robuster zu gestalten wurde eine API entwickelt, um den Monitor in bestehende Anwendungen zu integrieren, ohne dass Benutzer über spezifisches Monitoring-Wissen verfügen müssen. Um die Spezifikationssprache besser lernen zu können, wurde ein Tutorial entwickelt. Dieses Tutorial erklärt anhand mehrerer Beispiele die verschiedenen Operatoren der Sprache, gibt eine Übersicht über die zu Grunde liegenden Konzepte und beschreibt, wie man die Prototypen benutzen kann. Dieses Tutorial [4] wird im September auf einer internationalen Konferenz (International Symposium on Formal Methods) präsentiert und veröffentlicht.

Fehlertolerantes Monitoring (AP 2.3)

Dieses Arbeitspaket wird vom CISPA geleitet und vom DLR unterstützt. Aufgrund der Priorisierung von den neuen Use-Cases, die in dem Verlängerungsantrag eingeführt wurden, konnte dieses Arbeitspaket nur eingeschränkt abgeschlossen werden.

Eines der Ergebnisse in diesem Arbeitspaket sind ebenfalls die Module, die in dem AP 2.2 entwickelt wurden. Durch die Module können einzelne Subspezifikationen leichter getestet, gereviewed und verifiziert werden. Dies trägt dazu bei, dass weniger Fehler in der Spezifikation auftreten und auch Hardwarefehler leichter erkannt werden, wenn die gleichen Module unterschiedliche Ergebnisse liefern.

Außerdem wurde ein sehr vereinfachter Prototyp entwickelt, welcher die Spezifikation fehlerbehaftet auswertet. In einer fehlertoleranten Auswertung, wird angenommen, dass der Wert eines Inputstromes nicht korrekt ist und es kleinere Abweichungen geben kann. Diese Abweichungen können mit Intervallen angegeben werden, sodass Ouputströme nicht nur einzelne Wert berechnen, sondern Intervalle von Werten. Somit werden auch Triggerstrome unter einem Intervall ausgewertet und hat möglicherweise kein eindeutiges Ergebnis.

Traceable Monitoring (AP 2.4)

Dieses Arbeitspaket wird vom CISPA geleitet und vom DLR unterstützt.

Ziel dieses Arbeitspaketes ist die Entwicklung eines Prototypens für das AP 5.3 Zertifizierbarer Monitoringansatz. Dabei liegt der Fokus darauf einen Prototyp zu entwickeln der die Standards zur Softwareentwicklung einhält, sodass erste Schritte zu einer Zertifizierung des Prototyps gegangen werden. Eine generelle Zertifizierung wird im Rahmen des Projektes aber nicht angestrebt. Eine

Herausforderung in diesem AP liegt darin die Beziehung zwischen den Eigenschaften und dem ausführbaren Code zu dokumentieren. Im konventionellen Ansatz werden händisch Kommentare im ausführbaren Code eingefügt, die dokumentieren, welche Eigenschaft mit dem Codefragment implementiert wird. In diesem Projekt stellen wir eine Alternative vor, indem wir eine Spezifikation in der formalen Sprache RTLola, als Zwischenschritt einführen. Die Spezifikation hat eine wesentlich höhere Abstraktionsebene als eine Implementierung, sodass die Zuordnung zwischen den Eigenschaften und der Spezifikation wesentlich einfacher ist als zum ausführbaren Code. Im Projektzeitraum wurden die Spezifikationen von AP 3.2 vollständig dokumentiert und den entsprechenden Eigenschaften zugeordnet. Dafür wurden die Spezifikationen mit den entsprechenden Kommentaren ergänzt. Zusätzlich wurden in der Dokumentation der Eigenschaften die entsprechenden Stromnamen ergänzt, um auch diese Richtung zu dokumentieren. Durch das erhöhte Abstraktionslevel war eine sonstige Dokumentation nicht erforderlich. Die Beziehung zwischen dem resultierenden Code und der Spezifikation kann, während dem Erstellen des Codes automatisiert dokumentiert werden. Hierfür wurde ein neuer Prototyp, eine Kompilierung der Spezifikation, verwirklicht was dem Meilenstein dieses Arbeitspaketes entspricht. Dieser Prototyp wurde in Zusammenarbeit mit dem Arbeitspaket *Zertifizierbarer Monitoringansatz (AP 5.3)* verfeinert und konkretisiert und die generelle Idee wurde auf einer internationalen Konferenz veröffentlicht [8]. Außerdem entstanden im Projekt erste Ergebnisse für einen Translation-Validation-Approach. Mit diesem Ansatz wird verifiziert, dass die Semantik des Ausführbaren Codes der Semantik der Spezifikation entspricht. Dabei werden Annotationen geniert, die die Semantik der Spezifikation abbilden, welche von einem externen Verifikationstool überprüft werden können. Es ist nach dem Projektende geplant auch diese Ergebnisse bei einer Konferenz zu veröffentlichen.

Volocopter RV Integration (HAP 3)

Formalisierung der Spezifikationseigenschaften (AP 3.2)

Im Projektzeitraum konnten alle benötigten Eigenschaften in der Spezifikationssprache ausgedrückt werden. Diese Spezifikationen sind unter anderem in einem Repository gesichert und teilweise veröffentlicht [2]. Das CISPA unterstützte das DLR beim Formulieren der Eigenschaften und lehrte das DLR die Spezifikationssprache zu nutzen. Eine ausführliche Zusammenfassung der Ergebnisse wird vom DLR beschrieben.

Spezifikationsmanagement (AP 3.3)

Im Projektzeitraum wurde ein Konzept entwickelt, das Spezifikationen verschiedenen Abstraktionsebenen, welchen autonomen Softwareebenen entsprechen, zuordnet. Auf der niedrigsten Abstraktionsebene steht das „Item-Level“, welchen Eigenschaften wie: „Ein Sensor X muss 10-Werte pro Sekunde produzieren.“ abdecken. Auf der obersten Ebene steht das „Operation-Level“, welche Eigenschaften zusammenfasst die Missionen validiert. Solch eine Eigenschaft ist Geofenceing, welche überprüft, dass die Drohne in einem vordefinierten Bereich fliegt. Im Papier wurden verschiede Monitoreigenschaften gruppiert, wie temporale Eigenschaften oder statistische Eigenschaften, und für eine Gruppe und Abstraktion ein Beispiel gegeben. Zusätzlich wurden die Vor- und Nachteile einer formalen Spezifikationssprache diskutiert und zusammengefasst. Eine ausführlichere Beschreibung dieses Konzeptes kann im veröffentlichen Papier [7] gefunden werden.

Außerdem wurde ein Konzept entwickelt, welches statisch Eigenschaften einer Spezifikation überprüft, erweitert. Zusätzlich wurde der Ansatz um eine Laufzeitüberwachung erweitert, welche Eigenschaften dynamisch überprüft, wenn Annahmen über das System nicht mehr erfüllt sind. Eine ausführlichere Beschreibung dieses Konzeptes kann im veröffentlichen Papier [6] gefunden werden.

Zertifizierungsaspekte (HAP 5)

Zertifizierungsbarer Monitoringansatz (AP 5.3)

Dieses Arbeitspaket wird vom DLR geleitet und vom CISPA unterstützt.

Der Monitor ist eine sicherheitskritische Komponente des Luftfahrzeugs-Gesamtsystems. Daher gelten für den Monitor die typischen Anforderungen für die Zertifizierung. In diesem Arbeitspaket wird untersucht, was genau diese Anforderung sind und wie diese auf den Monitor heruntergebrochen werden können. Das CISPA bringt eine wissenschaftliche Perspektive und unterstützt das DLR bei der Recherche. Als Entwickler der Spezifikationssprache und der Prototypen informieren wir die Partner bei den Diskussionen, welche Anforderungen an den Prototypen bzw. per Design in der Sprache, wie zum Beispiel die Bestimmung des benötigen Speichers, umgesetzt sind. In diesem Arbeitspaket wird in erster Linie der entwickelten Prototypen von AP 2.4 benutzt. In den Diskussionen wird über den Fortschritt des Prototyps berichtet und mit Hilfe der Partner werden Verbesserungen an diesem Vorgenommen. Dabei werden Standards zur Softwareentwicklung wie DO-178C durchgearbeitet und auf die Implementierung der Prototypen übertragen. Im Projektzeitraum konnten die Ergebnisse auf einer internationalen Konferenz veröffentlich und präsentiert werden. Weitere Details sind im veröffentlichten Papier [8] zu finden.

Wichtigste Positionen im zahlenmäßigen Nachweis

Die Positionen im zahlenmäßigen Nachweis beziehen sich auf Personalkosten (Position 0812: 321.908,73) und Reisekosten (Position 0846: 3.403 EUR). Entgegen der ursprünglichen Planung gab es keine Ausgaben für internationale Reisen. Die Veröffentlichungen wurden aufgrund der Pandemie teilweise auf virtuellen Konferenzen vorgestellt oder wurden erst nach Projektende bei internationalen Konferenzen eingereicht. Außerdem gab es entgegen der Planung keine eigenen Investitionen, da die beantragten Entwicklungsboards von den Projektpartnern ausgeliehen wurden. Die bewilligten Mittel wurden für Personalmittel verwendet.

Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die Förderung des Projekts umfasst eine dreijährige Promotionsstelle in Vollzeit. Diese Stelle wurde auf 2 Mitarbeiter aufgeteilt und mit der Finanzierung entstanden 7 Veröffentlichungen auf internationalen Konferenzen. Außerdem wurden mehrere Prototypen implementiert. Zwei Prototypen wurden bereits veröffentlicht, die Veröffentlichung von weiten Prototypen ist geplant.

Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans

Die Verwertungsperspektive besteht aus Veröffentlichungen in internationalen Fachmedien um, die Notwendigkeit der Statusüberwachung zur Laufzeit basierend auf einer formalen Spezifikationssprache einem breiteren Publikum nahezulegen. Im Projektzeitraum entstanden 7 Veröffentlichung die schon auf internationalen Konferenzen veröffentlich wurden. 3 Veröffentlichungen sind ebenfalls noch nach dem Projektende geplant. Eine Liste aller Veröffentlichungen ist im letzten Abschnitt veröffentlicht.

Darüber hinaus entstanden im Projektzeitraum 6 Abschlussarbeiten mit denen Studenten in Kontakt mit der Thematik kamen und entsprechende Kernkompetenzen erlangten, um die Forschung fortzuführen.

Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens

Im Projektzeitraum ist eine detaillierte Übersicht über das Gebiet der Laufzeitüberwachung entstanden. Diese Übersicht findet man im Zwischenbericht Januar 2021 – Dezember 2021. Darüber hinaus gab es verschiedene Veröffentlichungen auf internationalen Konferenzen wie bei der International Conference on Computer-Aided Verification oder bei der International Conference on Runtime Verification.

Erfolgte oder geplante Veröffentlichungen des Ergebnisses

Im Rahmen des Projektes sind 7 Veröffentlichungen und Vorträge bei internationalen Konferenzen entstanden. Nachfolgend ist eine Übersicht:

- Automatic Optimizations for Runtime Verification Specifications @MT@CPSWeek2021 [4]
- RTLola: Formal Monitoring for CPS @FMR@IROS2021 [1]
- A Hierarchy of Monitoring Properties for Autonomous Systems@SciTech2022 [7]
- Monitoring with Verified Guarantees@STTT2022 [6]
- Monitoring Unmanned Aircraft: Specification, Integration, and Lessons-learned@CAV2024 [2]
- Certification Aspects of Runtime Assurance for Urban Air Mobility@SciTech2024 [8]
- A Tutorial on Stream-based Monitoring @FM2024 [5]

Darüber hinaus ist eine weitere Veröffentlichung mit dem Titel „Type-safe Monitoring of Parameterized Streams“ [3] konkret geplant, sowie zwei weitere Veröffentlichungen. Außerdem entstanden 6 Abschlussarbeiten die in der Bibliothek der Universität des Saarlandes veröffentlicht sind.

Bibliography

[1] J. Baumeister, „RTLola: Formal Monitoring for CPS,“ in *Transforming Specifications into Robot Programs: A Survey of Formal Methods Tools for Non-Experts*, Virtual, 2021.

[2] J. Baumeister, B. Finkbeiner, F. Kohn, F. Löhr, G. Manfredi, S. Schirmer und C. Torens, „Monitoring Unmanned Aircraft: Specification, Integration, and Lessons-learned.," in *36th International Conference on Computer Aided Verification.*, Canada, 2024.

[3] J. Baumeister, B. Finkbeiner, F. Kohn und M. Schwenger, „Type-safe Monitoring of Parameterized Streams".

[4] J. Baumeister, B. Finkbeiner, M. Kruse, S. Oswald, N. Passing und M. Schwenger, „Automatic Optimizations for Runtime Verification Specifications," in *6th Workshop on Monitoring and Testing of Cyber-physical Systems*, Virtual, 2021.

[5] J. Baumeister, K. Florian, B. Finkbeiner und F. Scheerer, „A Tutorial on Stream-based Monitoring," in *26TH INTERNATIONAL SYMPOSIUM ON FORMAL METHODS*, Milan, 2024.

[6] J. Baumeister, J. Dauer, B. Finkbeiner und S. Schirmer, „Monitoring with Verified Guarantees," *International Journal on Software Tools for Technology Transfer,* pp. 593 - 616, 2023.

[7] S. Schirmer, C. Torens, J. Dauer, J. Baumeister, B. Finkbeiner und K. Rozier, „A Hierarchy of Monitoring Properties for Autonomous Systems," in *AIAA SciTech Forum*, National Harbor, MD, USA, 2023.

[8] C. Torens, P. Nagarajan, S. Schirmer, J. C. Dauer, J. Baumeister, F. Kohn, B. Finkbeiner, F. Löhr und G. Manfredi, „Certification Aspects of Runtime Assurance for Urban Air Mobility," in *AIAA Aviation 2024 Forum,*, Orlando, 2024.

Berichtsblatt

1. ISBN oder ISSN	**2. Berichtsart (Schlussbericht oder Veröffentlichung)** Schlussbericht
3. Titel Volocopter Sicherheits-Technologie zur robusten eVTOL Flugzustands-Absicherung durch formales Monitoring – VoloSTreAM Robuste Laufzeitüberwachung mittels nachvollziehbarer Zustandsanalyse – RTLola	
4. Autor(en) [Name(n), Vorname(n)] Jan Baumeister, Bernd Finkbeiner	**5. Abschlussdatum des Vorhabens** 29.02.2024
	6. Veröffentlichungsdatum
	7. Form der Publikation Document Control Sheet
8. Durchführende Institution(en) (Name, Adresse) CISPA - Helmholtz-Zentrum für Informationssicherheit gGmbH Stuhlsatzenhaus 5, 66123 Saarbru¨cken, Germany	**9. Ber.-Nr. Durchführende Institution**
	10. Förderkennzeichen 20Q1963C
	11. Seitenzahl 6
12. Fördernde Institution (Name, Adresse) Bundesministerium für Wirtschaft und Klimaschutz (BMWK) 53107 Bonn	**13. Literaturangaben**
	14. Tabellen
	15. Abbildungen
16. DOI (Digital Object Identifier)	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Das übergeordnete Ziel des Verbundvorhabens „voloSTREAM“ ist die automatische Überwachung sicherheitsrelevanter Aspekte eines hochautomatisierten elektrischen Luftfahrzeugs. Ziel des CISPA-Anteils ist die Erforschung von theoretischen Grundlagen zur Laufzeitüberwachung unter Berücksichtigung von Fehlertoleranzen. Die Grundlagen werden in mehreren Prototypen realisiert. Diese werden für Flugversuche von dem DLR in einen Volocopter integriert. Der letzte entwickelte Prototyp soll nicht nur fehlertolerant, sondern auch nachvollziehbar sein. Dies ebnet den Weg zu einer Zertifizierung durch die EASA und somit einer industriellen Anwendung.	
19. Schlagwörter	
20. Verlag	**21. Preis**

Nicht änderbare Endfassung mit der Kennung 2418483-3

Document control sheet

1. ISBN or ISSN	**2. type of document (e.g. report, publication)** Veröffentlichung (Publikation)
3. title Volocopter Sicherheits-Technologie zur robusten eVTOL Flugzustands-Absicherung durch formales Monitoring – VoloSTreAM Robuste Laufzeitüberwachung mittels nachvollziehbarer Zustandsanalyse – RTLola	
4. author(s) (family name, first name(s)) Jan Baumeister, Bernd Finkbeiner	**5. end of project** 29.02.2024
	6. publication date
	7. form of publication Document Control Sheet
8. performing organization(s) name, address CISPA - Helmholtz-Zentrum für Informationssicherheit gGmbH Stuhlsatzenhaus 5, 66123 Saarbru¨cken, Germany	**9. orginators report no.**
	10. reference no. 20Q1963C
	11. no. of pages
12. sponsering agency (name, address) Bundesministerium für Wirtschaft und Klimaschutz (BMWK) 53107 Bonn	**13. no. of references**
	14. no. of tables
	15. no. of figures
16. DOI (Digital Object Identifier)	
17. presented at (title, place, date)	
18. abstract The overarching goal of the joint project “voloSTREAM” is the automatic monitoring of safety-relevant aspects of a highly automated electric aircraft. The aim of the CISPA part is to research the theoretical principles of runtime monitoring, taking fault tolerances into account. The basic principles are realized in several prototypes. These will be integrated into a Volocopter by DLR for flight tests. The last prototype developed should not only be fault-tolerant, but also traceable. This smooths the way for certification by EASA and thus industrial application.	
19. keywords	
20. publisher	**21. price**

Nicht änderbare Endfassung mit der Kennung 2418489-3